EXHIBIT 19

JBX Analysis Report

General Information

Analysis ID:	25393
Start time:	13:47:02
Start date:	09/11/2012
Overall analysis duration:	0h 3m 20s
Sample file name:	vm_tricks_sample
Cookbook file name:	default.jbs
Analysis system description:	XP SP3 (Office 2003 SP2, Java 1.6.0, Acrobat Reader 9.3.4, Internet Explorer 8)
Number of analysed new started processes analysed:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
SCAE enabled:	true
SCAE success:	true, ratio: 98%
Warnings:	• Too many NtQueryDirectoryFile calls (excessive behavior) • Too many NtProtectVirtualMemory calls (excessive behavior)

Classification / Threat Score

Persistence, Installation, Boot Survival:

Hiding, Stealthiness, Detection and Removal Protection:

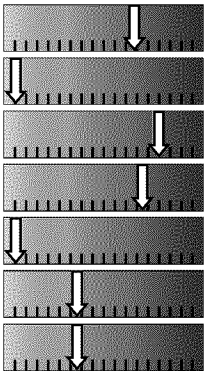
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection:

Spreading:

Exploiting:

Networking:

Data spying, Sniffing, Keylogging, Ebanking Fraud:



Matching Signatures

Behavior Signatures

Creates files inside the user directory
Queries a list of all running processes
Spawns processes
Urls found in memory or binary data
Binary may include packed or crypted data
Checks if the current process is beeing debugged
Creates files inside the system directory

Behavior Signatures

Creates mutexes	\BaseNamedObjects\Local\c:!documents and settings!networkservice!local settings!temporary internet files!content.ie5! \BaseNamedObjects\Local\c:!documents and settings!networkservice!cookies! \BaseNamedObjects\Local\c:!documents and settings!networkservice!local settings!history!history.ie5!
Drops PE files	
Enumerates the file system	
Found strings which match to known social media urls	
May tried to detect the virtual machine to hinder analysis (VM artifact strings found in memory)	
PE sections with suspicious entropy found	
Performs DNS lookups	
Posts data to webserver	
Tries to load a missing dll	ssleay32.dll libeay32.dll libssl32.dll
AV process strings found (often used to terminate AV products)	
Binary contains a suspicious time stamp	
Checks for available system drives (often done to infect USB drives)	
Contains capabilities to detect virtual machines	
Creates an autostart registry key	
Creates autorun.inf (USB autostart)	
Modifies the context of a thread in another process (thread injection)	

Code Signatures

Contains functionality to download additional files from the internet
Contains functionality to enumerate / list files inside a directory
Contains functionality to query local / system time
Contains functionality to start windows services
Contains functionality to dynamically determine API calls

Startup

- **system is xp**
- vm_tricks_sample.exe (PID: 656 MD5: 6B16C4526A013E744B3D91CD7A091C36)
  - vm_tricks_sample.exe (PID: 608 MD5: 6B16C4526A013E744B3D91CD7A091C36)
- svchst.exe (PID: 1084 MD5: 6B16C4526A013E744B3D91CD7A091C36)
  - svchst.exe (PID: 1356 MD5: 6B16C4526A013E744B3D91CD7A091C36)
- **cleanup**

Created / dropped Files

File Path	MD5
C:\Documents and Settings\NetworkService\Local Settings\Application Data\sLT.exf	D5AB441BD47EDE42EF7FBDB58D6DA541
C:\WINDOWS\mssys.dll	879631FB71EEF07DB32A97E8DAD372EA
C:\WINDOWS\svchst.exe	6B16C4526A013E744B3D91CD7A091C36
C:\autorun.inf	22E7E2047F46662384F91EAC7EFCC806
\ROUTER	C485FFBBCB652D92B63F1BF3301D6609
\net\NtControlPipe20	8E48D13549E3A7D91FFA1925918CBEDD

Contacted Domains

Name	IP	Name Server	Active	Registrar	e-Mail
mahaajan.in	208.91.198.109	ns2.md-4.webhostbox.net ns1.md-4.webhostbox.net	true	Directi Web Services Pvt. Ltd. (R118-AFIN)	support@vikcon.in
http://mahaajan.in/dd/	unknown	unknown	false	unknown	unknown

Contacted IPs

IP	Country	Pingable	Open Ports
208.91.198.109	unknown	true	21 80 443
195.186.1.121	SWITZERLAND	false	
195.186.4.121	SWITZERLAND	false	